Manual on the Proper Use of Email

Employee's guide to the protection of privacy when using email

apdcat
Autoritat Catalana de Protecció de Dades

Generalitat de Catalunya

Index

Tutorial appendix

How to sign and encrypt an email message

☐ DEFINITIONS

Email:	a messaging system which allows the transmission of messages between users without their needing to be connected at the same time.
Email address:	a set of words or symbols that identify the sender or recipient of an email message.
User:	a person who uses computer programs, in this case the email system.
Email account or email address:	a space facilitated by an email service provider where email messages are sent, received and stored.
Email service provider:	a company that offers the email service. The provider assigns an email address which can be accessed by means of a username and password.
IP address:	a number that enables the identification of computers in a network, such as the Internet.
Company:	in this guide, the term *company* is used to refer to all organisations that fall within the Catalan Data Protection Authority's scope of action.

What is an email address?

It is the set of freely-chosen words or symbols that identify a mailbox where email messages are received and sent:

Username
Identifies the email mailbox

@ the "At" sign
We can easily recognise an email address because it always contains the @

Domain
Identification facilitated by the email service provider

jordi @ llibreters.cat

Is the email address a personal data?

Personal data:

☐ Personalised addresses

The email address directly identifies the account holder (with the name, surname, initials, post, identification number, etc.) and must therefore be considered personal data.

joanidentitat@gencat.cat
E.C@gencat.cat
Directora@gencat.cat
000000000857346@gencat.cat

Note!

The fact that an address is personalised does not mean the email can be used for private purposes. You should refer to the rules for use of the corporate email system to ascertain whether personal use is permitted.

☐ Non-personalised addrwesses

In this case, the address does not directly identify the email account holder:

Akatombe80@gmail.com
Abc123@terra.net

Even though the address does not in itself identify the account holder (it employs an alphanumerical combination which is abstract or has no particular significance), it can make them easily identifiable:

- Because the address may appear alongside other data that enable the identification.
- Through the message content.
- Without inordinate effort, by means of the data held by the email server.

Non-personal data:

☐ Generic addresses

The email address corresponds, for example, to a service, activity or area of the organisation:

enquiries@gencat.cat

In these cases, the information provided by the email address is not linked to an identified or identifiable individual. It cannot, therefore, be considered personal data. It is often attended to by various, previously established users.

Note!

Employees and the people who communicate with accounts linked to these addresses should have no expectations whatsoever of privacy.

☐ Can my professional email address be published in my company's corporate directory without my consent?

Yes, for strictly professional purposes and only in those cases in which it is necessary, in accordance with the duties assigned to the employee. Otherwise, the address can only be published on the intranet.

What email systems can we use?

Email is an interpersonal messaging service which allows the transmission of messages between users without their needing to be connected at the same time. There are various applications that manage emails and which can be grouped, basically, into two categories:

☐ Email client

- These are programs that manage the sending and receipt of messages (e.g. Outlook, Outlook Express, Eudora, Mozilla Thunderbird, etc.
- The program downloads all messages and stores them in the computer memory, without detriment to certain protocols (e.g. IMAP) that can hold them on the server.
- The program can be installed in different devices (desk-top computer, laptop, smartphone, tablet, etc.).

☐ Webmail

- While still being able to receive messages through an email client, this system also allows the email server to be accessed via an Internet browser and the http or https protocol.
- It enables the sending and receipt of messages from any location via the Internet.
- The messages are stored in the server where the email account is located.

Note!

Email servers may be located in third countries which perhaps lack an acceptable level of personal data protection and, especially in the case of webmail, their conditions of use are established and modified unilaterally by the provider.

When the services are offered free of charge, remember:

- These conditions usually include authorisation for the processing of information managed by the provider for advertising or other purposes.
- The servers also frequently carry out automatic analysis of message content, which may be useful, for instance, in detecting viruses. The providers can also, however, use the information to send, in the same mail application, advertisements related to the message or other circumstances.

☐ Can I use the company email for private purposes?

- In cases where the rules for the use of email established by the company allow a degree of personal use, this should not be abused.
- Do not use the professional email address for personal business.
- Include the private or personal nature of messages in their title, or employ some other expression that enables the company to deduce this condition, in case it becomes necessary to access the email account.
- Delete any private information stored in the company-allocated email accounts as soon as possible. This is particularly important when you are going to be absent from your workplace for a long period of time (holidays, travelling, hospital admissions, etc.).
- If you are a union representative in your company you may use the email system to circulate union information to the other employees, providing this does not hinder the company's normal activity.

☐ Can the company access my email account?

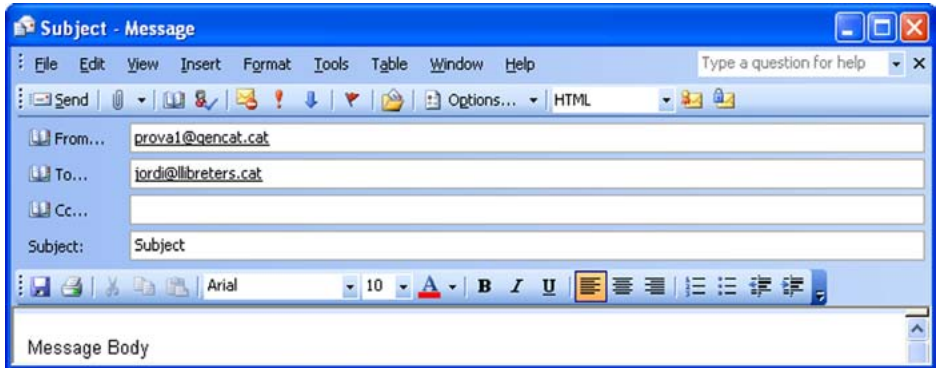
The company may only access corporate email accounts allocated to their employees when this is justified and there is no other mechanism available which enables the objective to be achieved without resorting to such access.

Access must be carried out in accordance with the rules for the use of email previously approved by the company, which should provide information on the mechanisms employed for monitoring the use of technologies which may affect individuals' privacy, and the consequences that may derive from improper use.

Remember

- Consult the company rules for the use of email to find out:
  - Whether use of the professional email address for private purposes is allowed.
  - Whether the company will provide employees with an email account for personal use.
  - Whether the company allows employees to use their own email account for personal purposes during working hours.
- The use for communications related with company activity of email accounts provided by servers other than those designated by the company should be avoided.

What elements make up an email?



☐ Email address of the sender and recipient

The email address can often easily be linked to a natural person. On occasions, the address itself facilitates such identification. In other cases, identification of the person who is its owner appears in the field corresponding to the address, together with it or even replacing it.

☐ Subject

The subject line should describe the nature or content of the message concisely and, if possible, without including personal details.

The confidentiality level of data included here will be lower than that of information contained in the message body, as simply viewing the inbox or outbox enables the subject to be read.

☐ Date and time of the email

The date and time of the email can also constitute personal data, since they allow us to establish the very moment it was sent and can even enable us to know where the sender was at that time.

☐ Message body

The body contains the content of the message, which can consist in formatted or unformatted text, or in images, which may include personal data. It may also contain links to websites or documents that contain personal information.

☐ Signature footer

This is the text that appears underneath the identification of the writer. It usually offers information about the sender's post and the organisation to which he or she belongs.

Email systems usually provide the option of automatically including a signature footer in messages.

☐ Attachments

Email systems enable users to attach images, documents, videos and audio to the message. The volume of personal information these attachments can include is extremely high.

Remember

- If the message is of a private nature and this cannot be deduced from the header, it should be indicated in the subject.
- Do not include personal information in the subject unless it is strictly necessary.
- Verify the email content, especially attached files, before sending it, to check the recipients' identity, confirm whether the data it contains can actually be sent and the security measures required.
- Avoid the communication of unnecessary identifying data when the content makes reference to third-party persons. If such communication is unavoidable, it should be made via an attached file.
- When the email message is of a private nature, disable the automatic signature footer option or, if necessary, delete from the footer any information relating to the post and organisation where the employee works.

Access to email: identification and authentication

In the rules for the use of email, the company should establish an appropriate policy on passwords to ensure the unmistakable, personalised identification of any user.

☐ Identification

Procedure to establish a user's identity, in this case that of the email user. A name is assigned to each user for this purpose.

☐ Authentication

Procedure to confirm a user's identity. In an email system this is normally done through the introduction of a password in addition to the user's identification, though other methods can also be used, such as a digital certificate.

☐ Password

Confidential information made up of a chain of characters. The strength of the password depends on the characteristics required for its establishment (password policy).

A **password** can be considered **strong** if:

- It contains at least 8 characters.
- It has been chosen at random and cannot be found in any dictionary.
- It can only be deduced by its user.
- Inordinate effort is needed to ascertain it.
- It includes letters, numbers, upper and lower case and, if permitted by the system, symbols.

A **password** can be considered **weak** if:

- It easily identifies the user.
- It has fewer than 8 caràcters.
- It is predetermined by the system or the system administrator.
- It is easily identifiable using dictionaries, or consists in proper names, significant dates, familiar numbers or simple variations of words.

Remember

- The first time you access the account, modify the default password generated by the system.
- Choose strong passwords. A personal access code which is difficult to decipher is the best guarantee of security.
- Keep the password safe. Do not make a note of it in an easily accessible place.
- Change the password with the regularity required by the system.
- The "security" questions you set in the forgotten password procedure should not require answers that could be discovered with a little investigation.
- Report any issue that might compromise system security immediately, following the established incident management procedure.
- Do not give the password to third-party persons, even if it is requested for system trials or similar purposes.
- Do not use the Remember Password option.
- Close the email session or block the computer when you leave the workplace, even briefly (e.g. with the Ctrl + Alt + Supr keys).

Best practices

When using the professional email account we must comply with applicable legislation as well as that established in the rules for the use of email laid down by the company. But beyond this, a number of best practices should be employed to ensure respect for other people's privacy.

When we want to write to more than one recipient.

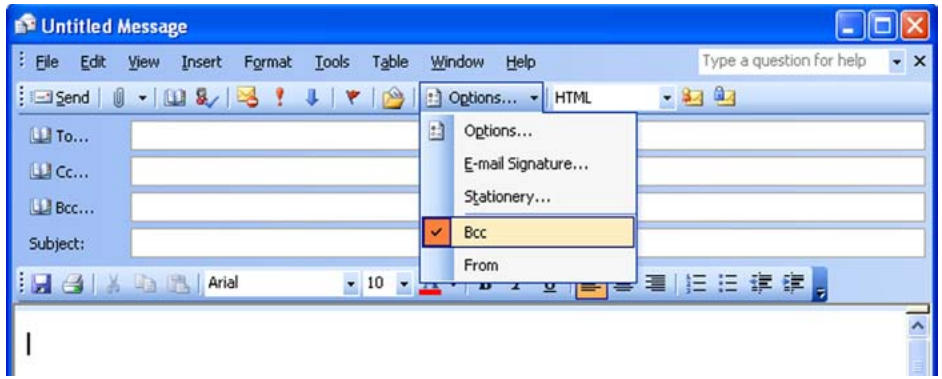
- Before answering an email that has been sent to various persons we should assess whether we need to send the reply only to the sender, or to all the other addressees too.
- The Respond to All option will make our message visible to all the people who appear in the address field as recipients.

What if we want to resend the email?

- Use the resend option only in those cases in which it is acceptable for both the sender and the message content, as well as all the information in the email thread, to be seen by the recipient.
- Do not participate in email chain letters. You may unintentionally make email addresses or contents available to third parties or contribute to spreading viruses or malware.

What is the blind carbon copy (Bcc)?

The Bcc (blind carbon copy) or Bc (blind copy) option ensures that emails addressed to various recipients do not reveal to the other recipients the addresses or identification of the persons entered in the Bcc field.



Remember

Use the Bcc option to avoid revealing the addresses of all your email's other recipients, especially if you do not have their consent or when no other circumstances exist that would allow such data to be made known.

By using this option you not only preserve the confidentiality of the other recipients, but also avoid receiving spam mail or similar.

You should remember however that some anti-spam filters may wrongly identify this type of messages, classifying legitimate emails as spam.

Can documents be attached to the email?

You should consult the company rules to see what kind of data communication can be made using email and, if necessary, attached files, who is authorised to do so and how the information received through this system should be treated.

Remember

- Before sending a file by email, analyse it to determine whether it contains personal data. If it does:
- Ensure that all the persons to whom you have addressed the email are entitled to access the information it contains, in accordance with their duties. Otherwise, do not send it. In the event the mail must be sent, select the information that each of the recipients will receive.
- Employ document encryption techniques in the case of data which, according to the RLOPD, requires a high level of security. Remember that emails and the documents attached to them are considered data supports for the purposes of the security measures to be applied in accordance with the aforementioned Regulation.

How can we guarantee our identity and the authenticity of our email content?

We can use a digital or e-signature to guarantee the authenticity and integrity of our communications. The e-signature is based on the digital certificate provided by the company and its conditions of use are established in the rules for the use of email:

☐ Digital signature

The digital signature is an integrated set of electronic data, linked and/or logically associated with other electronic data, which can be used by the signatory as their means of identification through a system of asymmetric cryptography. This mechanism authenticates the identity of the sender and the integrity of the message.

The digital signature can be generated on the basis of a digital certificate.

The company, with the collaboration if necessary of the Catalan Certification Agency (CATCERT), must provide its staff with digital signature systems which will identify the post-holder or their position and the administration or company in which they work.

You can see the steps to take to digitally sign an email at the following link:

We can use encryption to guarantee confidentiality:

☐ Encryption

Encryption consists in the transformation of a message using a code which makes it unreadable by anyone who does not have the decryption key. Encryption guarantees that the information is not intelligible or manipulated by third parties.

Data protection legislation makes encryption compulsory in the transmission of personal data over public networks or via wireless electronic data communication systems, when processing requires the application of high-level security measures:

- Data which reveal the ideology, trade union membership, religion, beliefs, racial or ethnic origin, health or sex life.
- Data obtained for police purposes without the consent of the data subjects.
- Data derived from acts of gender violence.

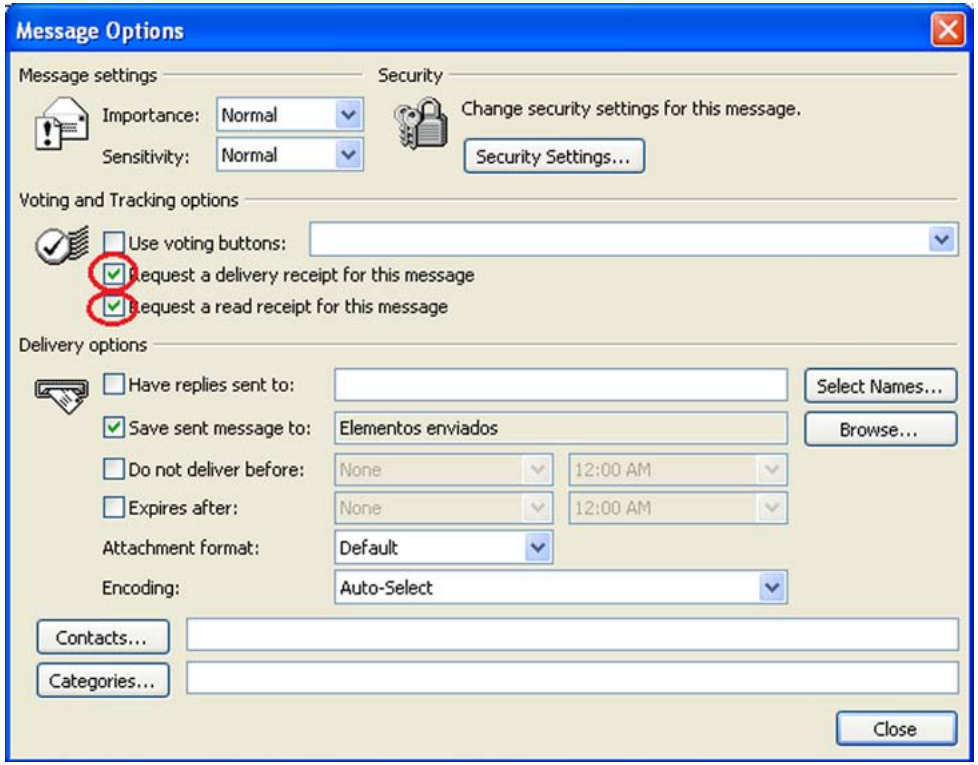
To decrypt a message you must have an encryption program installed in your computer and know the decryption key.

You can see the steps to take to encrypt an email at the following link:

How do we know our message has been received?

A mistake in the addressee's identification or in the email address can result in the message being received by someone other than its intended recipient. In such event, confidentiality of the email content will be compromised.

Email systems usually enable a Delivery Receipt and/or Read Receipt function to be activated. These options provide greater security, since they confirm the transaction has been completed successfully. However, we must always check the identification that appears in the receipt to ensure the message was received by the person for whom it was intended. It is also possible for the recipient to decline to send the receipt.



Remember

- Check the recipient's address before sending the email. The use of distribution lists is recommended (if the program has this feature) when the message is addressed to a previously configured group of users.
- Whenever possible, use the copy and paste option rather than typing addresses. This will avoid mistakes that can occur in rewriting them.
- Ensure you have the right recipients when selecting them from the company directory. Use the other information that appears alongside their name to make sure.
- Some programs automatically complete the address you are typing. If the address that appears is not familiar to you, check the completion in the Mail Contact Properties.
- Enable the Delivery Receipt and/or Read Receipt function before sending the message and, following a reasonable period of time, check the intended recipient has received it.
- You can include a pre-established text in the message footer that reminds recipients of the need to destroy the email if it has been received by mistake and to inform the sender of the error. The following may serve as an example:

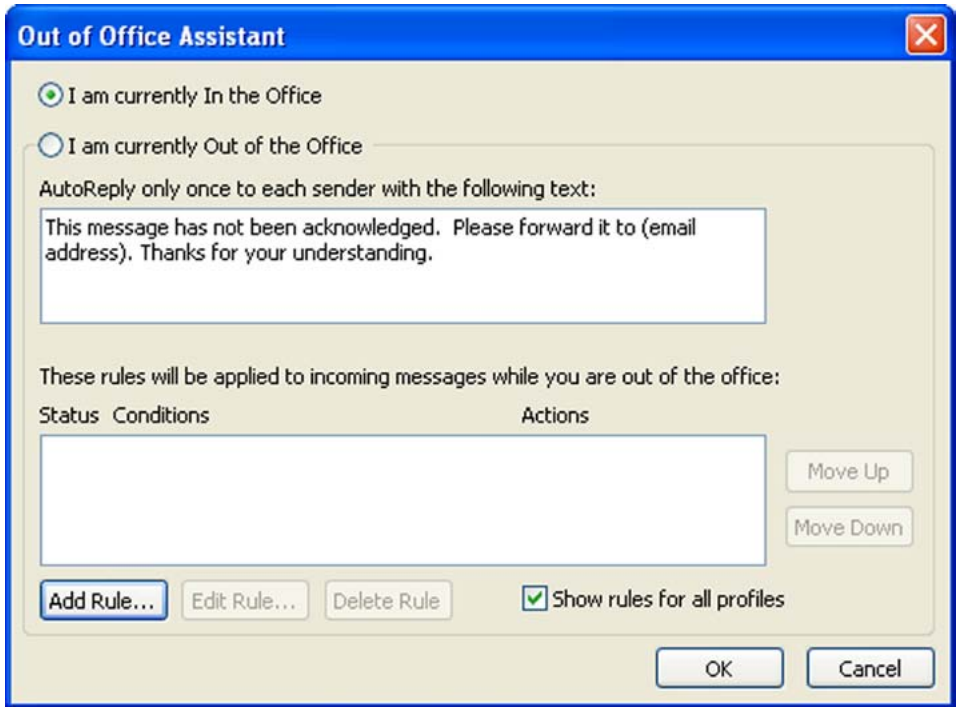
  "CONFIDENTIALITY WARNING

  This email may contain confidential information and is intended solely for the person or organisation to whom it is addressed. If you have received it in error please do not divulge its contents to third parties, but notify the sender and delete it from your system.

  Thank you."

Who can answer the emails when we are absent?

In the case of programmed absence, the automatic Out of the Office message can be enabled to respond to incoming emails.



☐ You should take the following considerations into account:

- The Out of the Office message enables people who send spam to validate your address as really existing.
- The content of the message may provide too much information to its recipient.
- On receipt of your Out of the Office message a third party could use this information to overload your mailbox with emails in an attempt to produce a Denial of Service (DoS) attack.
- In the case of absence, continuity of the service may require redirecting messages that arrive into your account to the address of another employee. If company rules for the use of email allow a certain amount of private use, you should inform your personal contacts of the new situation.

What if we want to access our email account from outside the office?

☐ Remote access

The company may authorise employees to access their email account remotely, through devices provided by the same company or personal equipment belonging to the employee or a third party, as well as via mobile technology such as laptops, smartphones, tablets and so on.

Remember

When using a shared-use computer to access email via webmail, you should:

- Use only secure protocols such as htpps.
- Delete your browsing history.
- Close the program every time you end a session.
- Do not enable the Remember Password option, to avoid it being registered in that computer.

☐ Access through mobile devices

Mobile devices must have the same security measures as fixed workstations, but the use of this type of email access may produce new problems which must be avoided.

Remember

- Comply with company security policies regarding users and passwords.
- Avoid using Wi-Fi networks you are not sure about.
- Only install in these devices applications that have previously been authorised by the head of security or other person designated for the purpose.
- Do not store sensitive information locally in these devices.
- In the event of loss or theft, immediately inform the company's head of security or the person designated for the purpose.
- Some devices can be configured so that the user or, if necessary, the email server, can remotely block access or find them in the case of loss or theft.

Junk mail or spam: how can we avoid it?

Bear in mind that advertising or promotional communications sent by email must have been expressly requested or authorised by the recipient, except when the following conditions exist:

- There is a prior contractual relationship to which the communication is linked.
- The address has been obtained by legitimate means.
- The communication refers to products or services from the same organisation which are similar to those that have been contracted.

Remember

- Do not respond to emails identified as spam or of dubious origin. Doing so will validate the address as existent and probably lead the receipt of more junk mail.
- Do not click on advertisements that appear in email messages that could be spam.
- Do not open attachments to messages from unknown senders without having previously scanned them with an anti-virus program.
- Do not use the Preview option.
- Be careful who you give your email address to.
- Avoid participating in chain messages.
- Send mesages using the blind carbon copy (Bcc) option.
- Delete addresses from the previous message when you resend an email.
- Do not publish the email address in search engines, forums, contact fields or websites, except when absoutely necessary.
- Install automatic spam or unsolicited mail filters.
- Use antivirus and anti-malware programs.
- Read the privacy policies and cancellation conditions carefully when contracting a product or service or making an online subscription in the performance of your duties.

Other security measures.

Remember

- Adapt the security options of your email account to the nature of the data you anticipate receiving or sending.
- Place or point the computer monitor in such a way as to protect the content of messages from the view of third-party persons who may be visiting the workplace.
- Do not install software not authorised by the company.
- Program the immediate elimination of messages that might contain viruses or malware. Complete elimination also requires their removal from the recycle bin.
- Inform the department responsible for IT security of any incident that may be detected in the system, in accordance with the protocol established by the company.